

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 12 of 25

REMARKS

In the Office Action mailed September 1, 2006, the Examiner rejected Claims 1-6, 15, 16, 19, 20 and 52-57 under 35 U.S.C.102(e) in view of Colosso (U.S. Patent 6,169, 976). Applicants respectfully submit that the rejection fails to establish the prima facie case of anticipation as each and every element of claims 1-6, 15, 16, 19, 20 and 52-57 are not taught or suggested by Colosso. See Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 U.S.P.Q.2D (BNA) 1913, 1920 (Fed. Cir.), cert. denied, 493 U.S. 853, 107 L. Ed. 2d 112, 110 S. Ct. 154 (1989) (explaining that an invention is anticipated if every element of the claimed invention, including all claim limitations, is shown in a single prior art reference). See Jamesbury Corp. v. Litton Industrial Products, Inc., 756 F.2d 1556, 1560, 225 USPQ 253, 256 (Fed. Cir. 1985) (explaining that the identical invention must be shown in as complete detail as is contained in the patent claim). See Verdegaal Bros., Inc. v. Union Oil Co., 814 F.2d 628, 631, 2 U.S.P.Q.2D (BNA) 1051, 1053 (Fed. Cir. 1987) (explaining that a prior art reference anticipates a claim only if the reference discloses, either expressly or inherently, every limitation of the claim). See Kloster Speedsteel AB v. Crucible, Inc., 793 F.2d 1565, 1571, 230 U.S.P.Q. (BNA) 81, 84 (Fed. Cir. 1986) ("Absence from the reference of any claimed element negates anticipation.")

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 13 of 25

In particular, Colosso does not disclose a method for providing cryptographic capabilities to a plurality of network users over a decentralized public network as recited in Claim 1. First, Colosso describes a web-based system that 1) receives a reported sale of a licensed software product to a particular customer and then 2) allows the customer to activate the software product and receive a key to turn on the software product. In short, the web-based system only operates as an authentication system. First, the web-based system authenticates the person as a valid customer and second, provides a key that authenticates the user inside of the licensed software. (Column 8, line 55 to Column 9, line 39; and Column 13, lines 7-19)

In contrast, the web-based system does not operate by “receiving a request for an access permission security profile on behalf of a network user” as recited in Claim 1. Indeed, the customer in Colosso requests a key and receives a key once they have properly authenticated themselves and their purchase of the licensed software. (Column 12, lines 65-67; Column 13-14, Column 15, lines 1-25.) The key requested in Colosso does not concern encrypting or decrypting objects to gain access but instead turning on a licensed software application. If the customer in Colosso wanted to access the licensed software, they could simply edit the software to view in a binary format or apply a reverse compiler to view the assembly code or source code. Of course,

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 14 of 25

the software application in Colosso could not be encrypted as it could not be executed on a computer and receive an activation key.

Indeed, it also follows that Colosso does not disclose or suggest, “creating the access permission security profile to be used in forming a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object and to encrypt selected portions of a plaintext object.” As previously described, Colosso is concerned about authenticating the customer as a valid licensee at a web-based system and then using a key to authenticate the same customer to the licensed software they have licensed for a fee. (Column 8, line 55 to Column 9, line 39; and Column 12, line 65 to Column 15, line 25). There is no mention of both encrypting the licensed software and decrypting the licensed software since the customer is interested in activating the software to execute certain functions. As previously mentioned, the customer in Colosso can readily look at the licensed software code in binary or source format but cannot make the code execute without the key.

Since Colosso is not encrypting or decrypting the licensed software with the keys, it also does not disclose or suggest, “securely transmitting the access permission security profile to the network user over the network” as recited in claim 1. As previously pointed out the “access permission security profile” in claim 1 is “to be used in forming a cryptographic key for enabling

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 15 of 25

the user to decrypt selected portions of an encrypted object and to encrypt selected portions of a plaintext object". In comparison, the key or keys transmitted in Colosso are keys and not "access permission security profile" as recited in Claim 1. Keys in Colosso are not access security profiles. The keys are also not used in forming a cryptographic key for both decrypting selected portions of an encrypted object and encrypting selected portions of a plaintext object. (Column 12, line 65 to Column 15, line 25). There is also no disclosure or suggestion in Colosso regarding encrypting or decrypting any selected portion of an object.

With regards to Claim 2, Colosso does not disclose or suggest that the creating step in Claim 1 comprises, "identifying one or more groups of network users who are to be provided with cryptographic capabilities; establishing one or more access codes for each group wherein each access code is adapted to be combined with other components to form a cryptographic key; and creating one or more security profiles for each network user, wherein each security profile contains at least one access code." Colosso describes providing keys to customers who have paid for a licensed product and have a valid customer account. (Column 13, lines 20-39.) There is no disclosure or suggestion in Colosso of creating a group of network users with cryptographic capabilities. Accordingly, Claim 2 is independently allowable as well as in condition for allowance by virtue of its dependence on allowable Claim 1.

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 16 of 25

It also follows that Colosso also does not disclose or suggest that each “group is a category, organization, organization unit, role, work project, geographical location, workgroup, or domain” as recited in Claim 3. As previously described, Colosso does not group customers together in groups but treats them as individual entities – groups of customers are not formed in Colosso as each customer is licensed individually. For example, each unique serial number provides a key to the key site manager that can be used to locate and retrieve customer information. (Column 11, line 57 to Column 12, line 18). Accordingly, Claim 3 is independently allowable as well as in condition for allowance by virtue of its dependence on allowable Claim 1.

Further, Colosso fails to anticipate a method for providing decryption capabilities to a plurality of network users over a decentralized public network as recited in Claim 4. First, Colosso does not disclose or suggest “receiving a request for decryption capabilities on behalf of a network user” as recited in Claim 4. Instead, the request received in Colosso is for a key that will activate a licensed product not for decryption capabilities. Any decryption that may occur subsequent to the request does not change the purpose of the request made in Colosso. (Column 12, lines 65-67 to Column 13, lines 1-6, Column 14, lines 56-64.)

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 17 of 25

Colosso also does not disclose or suggest “creating an access permission security profile to be used in forming a cryptographic key for enabling the network user to decrypt an encrypted object” as also recited in Claim 4. The access permission security profile describes at least one access code for each user. If two users have the same access rights, they will have the same access permission security profile. Accordingly, users having the same access permission security profile are able to decrypt the same object in the same manner.

In contrast, Colosso uses a first cryptographic key (referred to as an installation key) and a customer domain name to decrypt a second cryptographic key (referred to as an activation key) (Column 15, lines 45-52.) Clearly, no access permission security profile is used to decrypt the second cryptographic key. Moreover, the first cryptographic key or installation key is an alphanumeric string generated using a random number generator (Column 14, lines 65-67, Column 15, lines 1-5) and has no relationship to predetermined access permissions provided through an access permissions security profile.

Further, Colosso does not operate by “receiving from the user information associated with the encrypted object” as recited in claim 4. The only user information required by Colosso is a customer domain name but this is not associated with even an encrypted activation key or any

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 18 of 25

other object. Indeed, the encrypted activation key includes six fields of which the customer domain name is not mentioned. (Column 15, lines 1-5.)

Finally, the Colosso does not operate by “securely transmitting the cryptographic key to the network user over the network” as recited in Claim 4. As previously described, Colosso sends an installation key generated using a random number generator and an encrypted activation key created through a combination of six fields. (Column 14, lines 65-67, Column 15, lines 1-25.) Neither of these keys are a cryptographic key used directly to encrypt or decrypt any encrypted objects as recited in Claim 4.

For one or more of the reasons described above, Claim 4 remains in condition for allowance. Further, Claims 5 and 6 are in condition for allowance both independently and by virtue of their dependence on allowable Claim 4.

Colosso also does not disclose or suggest a centralized security management system for distributing cryptographic capabilities to a plurality of network users over a decentralized public network” as recited in Claim 52. Specifically, Colosso does not disclose or suggest “a set of client systems, wherein each client system includes means for receiving the requested member token and means for utilizing the cryptographic capabilities provided by the member token for selective encryption and decryption.” As previously described, Colosso is concerned about

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 19 of 25

authenticating the customer as a valid licensee at a web-based system and then using a key to authenticate the same customer to the licensed software they have licensed for a fee. (Column 8, line 55 to Column 9, line 39; and Column 12, line 65 to Column 15, line 25). There is no mention of both encrypting the licensed software and decrypting the licensed software since the customer is interested in activating the software to execute certain functions. In fact, the customer in Colosso may be able to look at the licensed software code in binary or source format but cannot make the code execute without the key. (Column 12, line 65 to Column 16, line 56).

For at least this reason, Claim 52 also remains in condition for allowance. Claims 53-58 also are independently allowable as well as allowable by virtue of their dependence on allowable Claim 52.

Claims 15-22 are not only allowable independently but also by virtue of their dependence on allowable Claims 1 and 4.

For at least these reasons above, the Applicants would respectfully request the Examiner to withdraw the rejection of Claims 1-6, 15, 16, 19, 20 and 52-57 under 35 U.S.C.102(e) in view of Colosso.

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 20 of 25

In addition, the Examiner rejected claims 7-11, 13-16, 19, 20, and 57 under 35 USC 103(a) over Colosso in view of Shanton (U.S. Patent 5,680,452).

“To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. In re Vaeck , 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)”

Applicants respectfully submit that Colosso does not disclose “a method for cryptographically securing the distribution of information over a decentralized public network to a plurality of network users” as recited in Claim 7. Specifically, Colosso does not operate by “creating one or more access permission credentials” as recited in Claim 7. Indeed, Colosso creates an installation key using a random number generator and an encrypted activation key using a set of six different fields but does not create access permission credentials. (Column 14, lines 65-67 and Column 15, lines 1-5.) First, installation key is generated randomly and not related access permission credentials. Second, the encrypted activation key references (1) the name of a product (2) historical data (3) OS platform (4) license level (5) names of modules (6) expiration dates. For example, these fields are assigned on a per customer basis in Colosso and

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 21 of 25

they do not ensure that only authorized users are able to decrypt encrypted embedded objects of the data object as recited in Claim 7.

Moreover, Colosso does not operate by “assigning an access permission credential to each of the selected embedded objects, wherein the access permission credential ensures that only authorized users are able to decrypt encrypted objects.” Indeed, Colosso uses creates an installation key generated using a random number generator and an encrypted activation key using a set of six different fields (Column 14, lines 65-67 and Column 15, lines 1-5.) Even if one of these keys was considered an “access permission credential”, there is nothing in Colosso that assigns one or both of these keys to a selected object or embedded object.

Even combining Colosso with Shanton does not teach or suggest each and every limitation of Claim 7. Even if Shanton did disclose embedded objects, Colosso does not assign the access permission credential to the objects or embedded objects. For the reasons previously described, Colosso does not use access permission credentials but instead uses an installation key generated using a random number generator and an encrypted activation key using a set of six different fields (Column 14, lines 65-67 and Column 15, lines 1-5.)

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 22 of 25

For one or more of the aforementioned reasons, Claim 7 remains in condition for allowance. Claims 8-14 and Claims 15-33 also remain in condition for allowance independently as well as directly or indirectly through their dependence on allowable independent Claim 7.

Accordingly, the Applicants respectfully requests that the Examiner withdraw the rejection of claims 7-11, 13-16, 19, 20, and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Colosso in view of Shanton and further in view of Kennedy and Win for failing to teach or suggest each and every claim limitation.

Claims 1-16, 18-22, 52, and 54-57 are rejected under 35 U.S.C. 103(a) over Halter (U.S. Patent 5,319,705) in view of Win (U.S. Patent 6,161,139).

Applicant respectfully submits that Halter does not disclose or suggest “a method for providing cryptographic capabilities to a plurality of network users over a decentralized public network” as recited in Claim 1. First, Haller does not disclose or suggest “receiving a request for an access permission security profile on behalf of a network user” as recited in Claim 1. Instead, Haller provides distributing a “unique customer key” and not an access permission security profile (Column 8, line 61 to Column 9, line 27). Indeed, Win also does not provide an access permission security profile in lieu of a unique customer key. Even if there were a motivation to combine Haller and Win, this particular limitation would not be met. For at least this reason

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 23 of 25

Claim 1 remains patentable over Haller in view of Win. Claims 4, 7 and 52 are allowable for at least the same or similar reasons as are dependent claims 2-3, 5-6, 8-14, 15-22, and 53-58 which depend directly or indirectly from one or more of the aforementioned allowable independent claims.

Moreover, Haller does not operate by “creating the access permission security profile to be used in forming a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object and to encrypt selected portions of a plaintext object” as recited in Claim 1. Haller does not disclose or suggest a cryptographic key capable of decrypting selected portions of an encrypted object and neither does Win. For at least this additional reason Claim 1 remains patentable over Haller in view of Win. Claims 4, 7 and 52 are allowable for at least the same or similar reasons as are dependent claims 2-3, 5-6, 8-14, 15-22, and 53-58 which depend directly or indirectly from one or more of the aforementioned allowable independent claims.

Further, Haller does not operate by “securely transmitting the access permission security profile to the network user over the network” as recited in Claim 1. Haller in fact teaches away from secure communication suggesting that the keys are delivered to a person orally over a phone (Column 9, lines 18-21). Clearly, Haller did not disclose, suggest or contemplate any form of secure communication and neither has Win. For at least this additional reason Claim 1 remains

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 24 of 25

patentable over Haller in view of Win. Claims 4, 7 and 52 are allowable for at least the same or similar reasons as are dependent claims 2-3, 5-6, 8-14, 15-22, and 53-58 which depend directly or indirectly from one or more of the aforementioned allowable independent claims.

In summary, Applicants respectfully request reconsideration and withdrawal of the rejections for claims 1-6, 15, 16, 19, 20 and 52-57 under 35 U.S.C.102(e), 7-11, 13-16, 19, 20, and 57 under 35 USC 103(a) and 1-16, 18-22, 52, and 54-57 are rejected under 35 U.S.C. 103(a).

///

///

///

///

///

///

///

///

///

///

///

Applicant : Sweet et al.
Atty Dkt. : 00131-000100000
Issued : n/a
Serial No. : 09/930,029
Filed : 08/14/2001
Page : Page 25 of 25

///

///

///

///

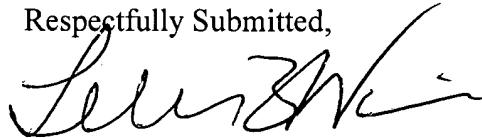
The Applicant has made a diligent effort to place the claims in condition for allowance, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Leland Wiesner, Applicants' Attorney at (650) 853-1113 so that such issues may be resolved as expeditiously as possible.

For these reasons provided above, this application is now considered to be in condition for allowance and such action is earnestly solicited.

March 1, 2007
Date

Wiesner and Associates
366 Cambridge Ave.
Palo Alto, California 94306
Tel. (650) 853-1113

Respectfully Submitted,



Leland Wiesner
Attorney/Agent for Applicant(s)
Reg. No. 39424